RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: IMT-M01

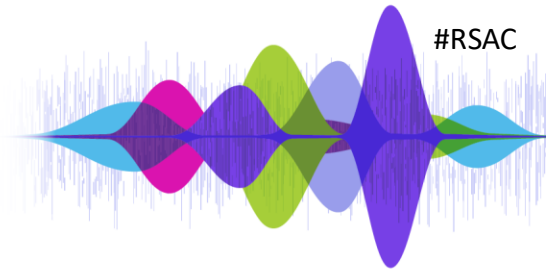
“We Work 5000 Hours” – One Bank’s Journey to Conquer Burnout in Cyber

Brenden Smith

Chief Information Security Officer
FirstBank

Emy Dunfee

Director – Security
FirstBank



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Introduction

Brenden Smith
20 years experience
Incident Horror Story – Narcotics accidentally “deposited” by a customer. Police declined to assist.

Emy Dunfee
22 years experience
Incident Horror Story –
Full DR due to a server room flooding, then starting on fire (in that order)

FirstBank Cybersecurity Personnel

- 132 year combined expertise
- Average tenure 6.9 years
- 1810 Splunk alerts received in 2024
- All hiring since December 2022 due to internal promotion or team growth
- 0 resignations since 2022

A Well Known Problem

- 2022 VMWare Global Incident Response Report lists Cybersecurity burnout as a critical issue "Forty-seven percent of incident responders said they experienced burnout or extreme stress in the past 12 months, down slightly from 51% last year. Of this group, 69% (versus 65% in 2021) of respondents have considered leaving their job as a result. Organizations are working to combat this, however, with more than two-thirds of respondents stating their workplaces have implemented wellness programs to address burnout." (https://news.vmware.com/releases/vmware-report-warns-of-deepfake-attacks-and-cyber-extortion)
- Addressing cybersecurity burnout is one of Gartner's Top Cybersecurity Trends for 2025 (https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025)
- At the RSA 2024 Conference, cybersecurity burnout and employee retention was a key area of focus

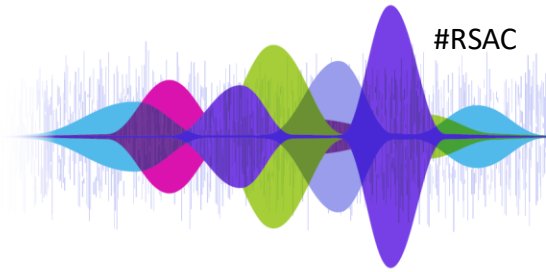
Flex Time

Global Outage of a Cybersecurity Endpoint Detection Tool

350 Hours Responding

- Flex time can be used like PTO, but does not pull from their PTO balance.
- For every 5 hours of incident time worked, an employee receives a full day of flex time.
- Working an incident over a weekend (no matter the length, within reason), an employee receives two days of flex time
- Flex time is also offered generously if an employee works an overnight incident

Flex Time

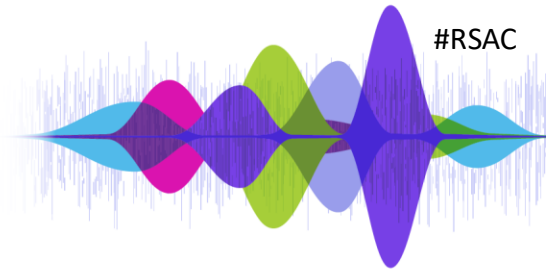


- Immediate acknowledgement of effort and time away from non-work priorities
- Works for any employee in any position
- Can be used in any increment (even an hour can be effective!)
- Will need to ensure the employee is truly logged off and disconnected

It’s important to also ensure employees are using PTO effectively throughout the year. Hoarding PTO can counteract the effective use of flex time.

Red Team Testing

Red Team Testing

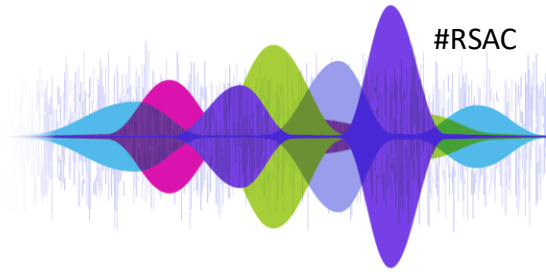


- Your teams need opportunities to be successful
- High false positive environments lead to:
  - Frustration/Anxiety
  - Lack of Closure
  - Encouragement of Bad Habits

Red Team Testing

- Physical security is a good parallel
- Stopping bank robberies is hard

Red Team Testing

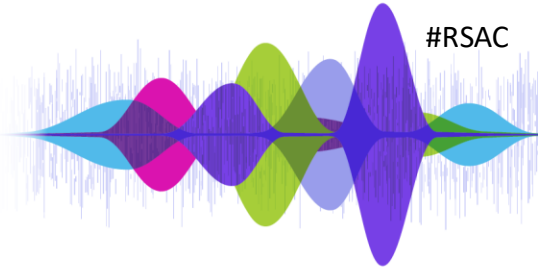


One Year of Credential Stuffing Activity

1,275 Hours Responding

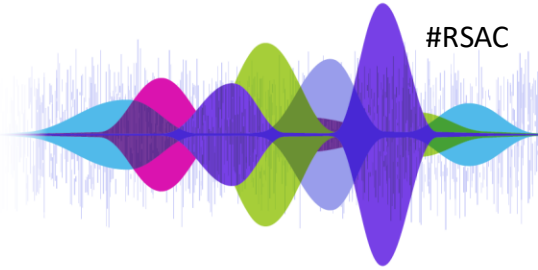
- Credential stuffing is time consuming and tedious to respond to
- Often requires off-hours work, leading to loss of sleep and poor work life balance
- Mitigation is usually incomplete, employee's don't get a "win"

Red Team Testing



- Use Red Team Testing to help your team get detection wins
- Your controls improve, and your team can celebrate their successful detections
- We use Continuous Red Team testing 24/7/365
- Pace of testing is balanced with burnout indicators
- RSA Talk: “Red vs. Bank: Surviving a Three Year Red Team”

Professional Development Opportunities

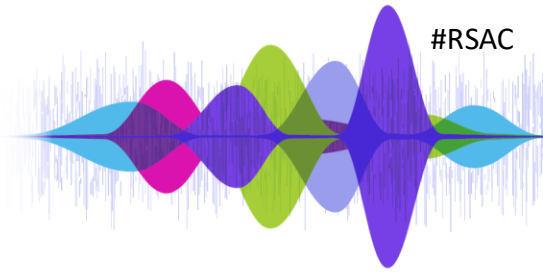


Smish Texts from Company Executive

36 Hours Responding

- Look for opportunity to reward incident effort with innovative or high value opportunities
- Attendance can be to a webinar, user group, major conference, minor conference, in town/out of town… the manager and employee choose together
- Doesn't have to be directly related to the employees current role or the incident

Professional Development



- If is directly related to the incident, quickly demonstrates support for filling knowledge or response gaps identified in that incident
- Opportunity to explore different areas of security OR do a deeper dive in an area the employee is passionate about
- Free passes readily available
- Investment in employee, department and organization

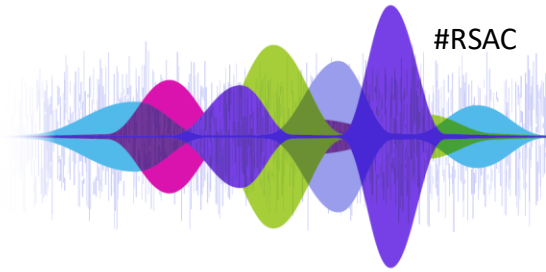
Team Mentality

- You need to have the best insight into your staff
  - Exit Interviews are OK, but get your own intel

Team Mentality

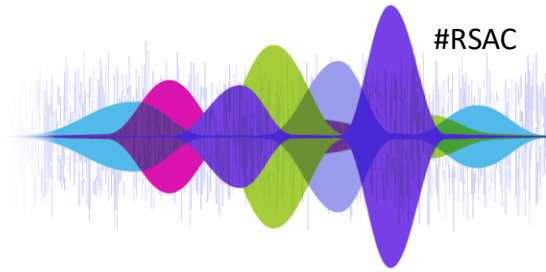
- Personnel Management
  - Security needs to be held to a high standard
- Team Advocacy
  - Hold your team to a high standard,
    and aggressively advocate for them

Team Mentality



- Risk Acceptance
  - Your team wants to run a strong program
  - Frustration builds when risks are “ignored” from their perspective
  - A clear understanding of Risk Acceptance and Risk Management concepts alleviates that frustration

Get Cheesy!

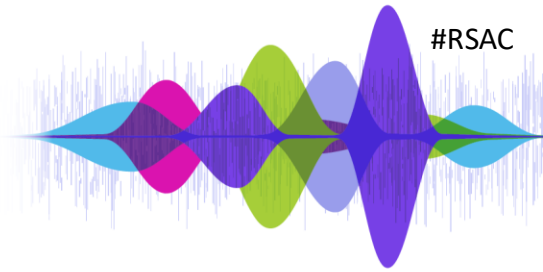


Personnel Management, Executive Communication, Split Second Decision Making, Calming the Masses

Never-ending ☺

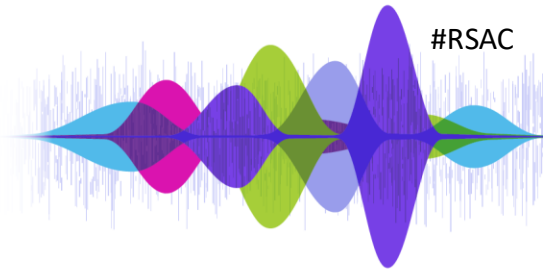
- Pizza parties!
  - When a manager achieves something “impossible” – they receive a homemade pizza party coupon to be redeemed at a time of their choosing. Pizza is then provided for the whole management team
- Make time for something not work related, but at work. A book club, card games, IM channels dedicated to memes/giphies….
- Provide food and beverages generously

Getting Cheesy!



- Be sure individuals know the “reward” is ironic and fun, but still real. Don’t only give pizza parties and never flex time
- Everyone loves free food and beverages! Plus it is easy to do for remote employees!
- These items do not have to be expensive or time consuming. Pokémon trivia for the title of “Trivia Genuis”…. You would be surprised what makes people engaged and relaxed
- Not one size fits all….. Know your employees and team dynamics…..

Takeaways to Apply



- Always look for opportunities highlight your cyber team with Senior Leadership
- Have an arsenal of training or conference opportunities ready to suggest for the team
- Know your teams! Be familiar with how they respond to stressful situations and know how best to motivate them
- Don’t be afraid to be creative! Silliness, humor, irony, cheesiness… if it works for the team, be open to it!
- True Appreciation Goes a Long Way. Don’t be stingy with the gratitude!

RSAC™ 2025 Conference

Many Voices.
One Community.

Brenden.Smith@efirstbank.com

Emy.Dunfee@efirstbank.com